Participants of the Lead Safe Hamilton County Home Repair program are required to submit personal and confidential information in order to participate. This information includes items such as: name, address, telephone number, social security number, birthdate, bank records, driver's license, etc. This document serves as LISC Greater Cincinnati, and our partners use of the information provided and our guarantee to protect your personal information.

This confidential information will be used for the following purpose(s):

- **Determining your eligibility for the Lead Safe Hamilton County Home Repair program.**

This confidential information may be shared for the following purpose(s):

- **To determine eligibility for the program, assess scope of work for your home and receive homeowner information for grant reporting purposes.**

This confidential information may be shared with the following entities or organization(s):

- **LISC Greater Cincinnati**
- **Working in Neighborhoods (WIN)**
- **Habitat for Humanity of Greater Cincinnati**
- **Ohio Department of Development**

This confidential information will not be shared or disseminated except as indicated above, unless explicitly approved by you, the participant.

By providing this confidential information in connection with this program, Lead Safe Hamilton County, you are agreeing to the terms and conditions outlined above. If at any time, you want to receive a copy of or change or opt out of (no longer want to participate) this program, you can do so by following the instructions below.

LISC strives to preserve data privacy and security. Access to all confidential information is strictly monitored and limited to only those who have a business need to such confidential information.
If you would like to receive a copy or update your confidential information/or opt out of this program, please follow the directions below.

Requests for a copy of either your confidential information or to opt out of this program must be made in person at the intake center. At the time you make your request, you will be asked to complete a form that will be forwarded to the appropriate parties at LISC. Once LISC receives your request, you should receive notification from LISC within thirty (30) days of receipt of such request.

For definitions of confidential information, please see back of this sheet.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as name, home address, telephone number, Social Security number (SSN), or biometric records (e.g., finger prints, DNA profile, voiceprints, etc.) alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date of birth or mother's maiden name. Also known as “personal information.”

Protected Health Information (PHI): A specific type of PII, as defined under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and associated amendments. PHI is a type of regulated personally identifiable information that relates to the past, present, or future physical or mental health of an individual, the provision of health care to an individual, or the payment for the provision of health care to the patient, and can be reasonably used to identify the individual. PHI includes a number of identifiers that are unique to an individual, including demographic, biometric and genetic information. All references to PII in this policy include PHI.

Sensitive PII: A subset of PII that if released would pose a higher risk of subsequent identity theft or personal harm. For example, an individual’s SSN is sensitive PII. Sensitive PII also includes an individual's name, home address, or telephone number in combination with any of the following:

- Government-issued identification number, such as a SSN, driver's license number, or Taxpayer Identification Number;
- Date or place (e.g., zip code) of birth;
- Financial account information, such as bank or credit card information, account numbers and balances, PINs, passwords, and security codes/questions;
- Biometric records;
- Medical Information protected under the Health Insurance and Portability Accountability Act of 1996; and/or
- Background investigations including reports or databases.